SARSAT

Configuration Management Plan

Version 2.1

1 April 2006

Table of Contents

List of Figures

List of Tables

List of Appendices

Cospas-Sarsat Operations
Configuration Management Plan

1 Introduction

The National Oceanic and Atmospheric Administration (NOAA)/National Environment Satellite, Data, Information Service's (NESDIS) Direct Service Division (DSD) operates the United States Mission Control Center (USMCC) and 14 satellite ground stations referred to as Local User Terminals (LUT). The LUTs and USMCC provide the United States ground segment of the international Cospas-Sarsat Program.

NOAA assumed responsibility of USMCC operations in 1990 with the second generation USMCC which operated on an IBM mainframe computer. Components of the USMCC function were transferred to a PC-based system in 1993. This system is now referred to as the third generation USMCC. As major portions of this system were proprietary to a third party vendor, only a limited configuration management system could be implemented. In 1998 the fourth generation USMCC began initial operations. The system is based on modular design and utilizes the concept of distributed processing. Functions are distributed on different processors operating on a Windows 2003 Network (LAN).

In August 2003, the 406 MHz Registration Data Base (RGDB) was migrated to a web based system that provides online access for beacon owners and Search and Rescue (SAR) users. This web applications network has further expanded to include an online version of the Incident History Data Base (IHDB). All hardware, application software, COTS, data files and documentation associated with the RGDB and IHDB are included as part of the USMCC Configuration Control domain.

Historically, a third party vendor has provided the equipment and the software necessary to perform the functions of Cospas-Sarsat LUTs. Although the software is controlled by the vendor, it is necessary to incorporate portions of the LUT system into this plan. This document is the Configuration Management Plan for the LUTs, the USMCC and all the communication equipment and links managed by the DSD to support the LUT and USMCC systems.

1.1 Purpose

The purpose of this plan is to provide detailed configuration management for hardware, software, and associated documentation related to the United States portion of the Cospas-Sarsat ground segment.

1.2 Scope

This plan applies to all documentation, computer source code, executable programs, data files, software development tools, hardware, operating systems, and processes used in support of the DSD’s Cospas-Sarsat mission.   Section 2 identifies the responsibilities of the persons involved with configuration management. Section 3 contains details on the items under configuration control. Although configuration management plans typically include all phases of the software development life cycle (design, testing, etc.), this plan only addresses operational software and documentation that has reached version 1.0 or higher. Section 4 describes the procedures used to initiate changes to DSD’s Cospas-Sarsat system. Section 5 describes the composition of the configuration control board and criteria used to accept and reject changes. Finally section 6 describes the process to track the disposition of configuration change requests.

1.3 IT Security

Information Technology (IT) security is an integral part of the configuration management of the USMCC. The Direct Services Division (DSD) Information System Security Officer (ISSO) is a permanent member of the Sarsat Configuration Control Board and ensures that IT security is considered in the USMCC change management process. As part of any proposal for system change, a risk assessment shall be performed to determine the security requirements. If the change proposal includes Commercial Off-the-Shelf (COTS) components, appropriate security requirements will be identified and included in the COTS acquisition plans.

As changes are made to the USMCC system, documentation shall be updated to include security controls. In addition, the Sarsat Security Plan will be reviewed for necessary changes resulting from approved changes to the USMCC system.

1.4 Definitions

The term “Baseline” is defined as a specification or product that has been formally reviewed and agreed upon, and serves as a basis for further development, which can be changed only through change management procedures. Baseline includes requirements, source code, executable programs, data files, hardware and associated documentation. These items collectively are also referred to as a “System.”

The term “Configuration Management” is defined as a process by which a system’s baselines are identified, controlled and tracked as changes occur or new components to the system are added. The term configuration control is also used to refer to configuration management.

The “USMCC” refers to all mission-critical or mission-support software and hardware systems in use by DSD to complete its mission.

“LUT” refers to the hardware and software systems provided by the LUT vendor for use by DSD. The software is proprietary to the LUT vendor and although the hardware equipment is owned by DSD, the configuration is controlled by the LUT vendor. Modifications to the software and hardware are coordinated with DSD.

The term “Corrective Maintenance” identifies software or hardware maintenance required to correct unexpected problems or to modify the system to meet existing requirements or specifications.

The term “Adaptive Maintenance” identifies system changes resulting from altered requirements in support of national or international initiatives, or planned changes in the processing environment (e.g., addition of new software or hardware, operating environment, data structures or software algorithms).

“Perfective Maintenance” identifies software and hardware maintenance required to improve the operation of the system in terms of efficiency, reliability, performance or maintainability of software.

1.5 References

Further information on configuration management can be obtained from the following sources:

a) “ISO 9000-3,” Raymond Kehoe and Alka Jarvis, Springer, New York, New York 1996.

b) “Software Engineering,” Ian Sommerville, Addison-Wesley Publishing Company, Reading Massachusetts, 1996.

c) “Implementing Configuration Management,” F.J. Buckly, IEEE Press, 1993.

d) Sarsat Security Plan

- End of Section 1 -

2 Configuration Management Responsibilities

All authority for managing the USMCC and LUTs is vested in the Chief of the Direct Services Division, and the Contracting Officer's Technical Representative (COTR) for the USMCC maintenance and operations contract, as well as the COTR for the LUT maintenance contract. Responsibilities for the key persons involved in the configuration management process for the USMCC and the LUTs are provided below.

Note that the same person may occupy more than one role, or one functional position may require more than one person. Maintenance and Operations personnel, and LUT Vendor personnel are typically contractors. Additionally, other personnel may be involved, as necessary, to assist the key staff identified below. The current personnel assigned to the configuration management process are identified in Appendix A.

Configuration Manager

The configuration manager is responsible for:

- scheduling configuration control board meetings;
- ensuring that all logs are current;
- reviewing change proposals and submitting them to the configuration control board;
- configuration control audits as necessary;
- ensuring correct configuration control procedures are followed; and
- generating and providing configuration control reports as required.

Information System Security Officer (ISSO)

The ISSO is responsible for:

- reviewing change proposals and problem reports to determine what, if any, impact the change/fix may have on the USMCC security configuration and policy
- making recommendations, if necessary, to appropriate Government personnel as to proposed changes/fixes to satisfy IT security policies.
- reviewing completed SCPs/SPRs to determine if the final change/fix that was implemented is compliant with all IT security policies applicable to the USMCC.

2.1 USMCC

SARSAT Operations Manager

Coordinates the development and implementation of USMCC systems to include:

- chairing the configuration control board meeting as required;
- approving of all modifications to the USMCC operation;
- approving of all modifications in the LUTs that impact the USMCC;

- managing the disposition and resolution of all system problem reports and system change proposals associated with the USMCC;
- assigning priority to outstanding system problem reports or system change proposals associated with the USMCC;
- developing any necessary standard operating procedures; and
- determining the requirements specifications of the USMCC.

Maintenance and Operations COTR

Responsible for the maintenance and operations vendor in terms of day-to-day contract performance, duties include:

- allocating resources;
- procuring additional resources as necessary;
- ensuring adherence to contract specifications;
- coordinating with vendor on software life-cycle management issues; and
- coordinating with vendor on hardware requirements, selection and procurement.

USMCC Chief

Responsible for the day-to-day operation of the USMCC, duties include:

- notifying/coordinating with other MCCs of system modifications as necessary;
- coordinating modifications with operations staff; and
- recommending schedules and priority for system modifications.

Maintenance and Operations Project Manager

Responsible for administrative issues related to maintenance and operations contractor, duties include:

- ensuring availability of resources;
- acting as point of contact for configuration management issues between vendor and DSD;
- managing subcontractors involved in system modifications; and
- assigning resources to tasks.

Maintenance and Operations Senior Analyst/Lead Programmer

The maintenance and operations senior analyst, along with the necessary programming staff, will be responsible for leading the design effort associated with any system modifications. In addition the senior analyst, analyst, lead programmer or programmer will also:

- provide time estimates for system change proposals;
- perform tasks to modify system code or system configuration;

- plan and perform all necessary testing;
- plan and perform all aspects of implementation associated with a system change; and
- complete etailed reporting associated with system problem reports or system change proposals.

2.2 LUTs

LUT Maintenance COTR

Coordinates the development and implementation of LUT systems to include:

- chairing configuration control board meetings as required;
- approving all modifications to the LUT system;
- managing the disposition and resolution of all system problem reports and system change proposals associated with the LUTs;
- assigning priority to outstanding system problem reports or system change proposals associated with the LUTs;
- developing any necessary standard operating procedures for the LUTs;
- managing the requirements specifications of the LUTs;
- managing the LUT vendor in terms of day-to-day contract performance;
- allocating resources associated with the LUT vendor;
- procuring additional resources as necessary;
- ensuring adherence to contract specifications;
- coordinating with vendor on software life-cycle management issues; and
- coordinating with vendor on hardware requirements, selection and procurement.

SARSAT Operations Manager

Coordinates the development and implementation of LUT systems that affect USMCC operations.

USMCC Chief

Responsible for the day-to-day operation of the USMCC, duties include:

- notifying/coordinating with other MCCs of system modifications as necessary;
- coordinating modifications with operations staff; and
- recommending schedules and priority for system modifications.

LUT Maintenance Vendor

Responsible for administrative and technical issues related to LUT maintenance as defined by contractual parameters, duties may include:

- ensuring availability of resources;

- acting as point of contact for configuration management issues between vendor and DSD;
- managing responsibility for any subcontractors involved in system modifications;
- assigning resources to tasks;
- providing time estimates for system change proposals;
- performing tasks to modify system code or system configuration;
- planning and performing all necessary testing;
- planning and performing all aspects of implementation associated with a system change; and
- completing detailed reporting associated with system problem reports or system change proposals.

- End of Section 2 -

3 Items Under Configuration Management

All base lined items are under configuration management. As described in section 1, a baseline is an official version of a product or documentation. Those items whose functional and performance parameters require strict control will be placed under configuration control. Also, those item's that interface with other components or external agencies (i.e., the Coast Guard or the Air Force) will be under configuration management. In order to identify items under configuration management, the following general guidelines were followed:

a) whether the component is considered mission critical, mission support, or operational by DSD or NESDIS;
b) the ability to uniquely identify an item; and
c) the requirement for approval.

This section provides details on which items are base lined, therefore under configuration management. Appendix B describes the current DSD systems and sub-systems under configuration management. The relationship between application software, hardware, operating systems, and commercial products is described in the USMCC Functional Description Document (FDD).

3.1 USMCC

3.1.1 Application Software

Software used by the USMCC to produce, or support data distribution is subject to configuration control. This includes, but is not limited to:

- all C++, Fortran, Visual Basic and SQL source code;
- all ASCII and SQL configuration files with the exception of those listed in section 3.1.7;
- all header/include files;
- all executable code;
- all stored SQL procedures;
- all scripts/macros;
- timer and triggers
- all SQL Server Views; and
- all batch files.

Application software is stored in the appropriate directories as identified in Figure 3.1. Access to the software directories is limited to appropriate personnel. Application software will be modified according to the standards contained in *[TBD]*.

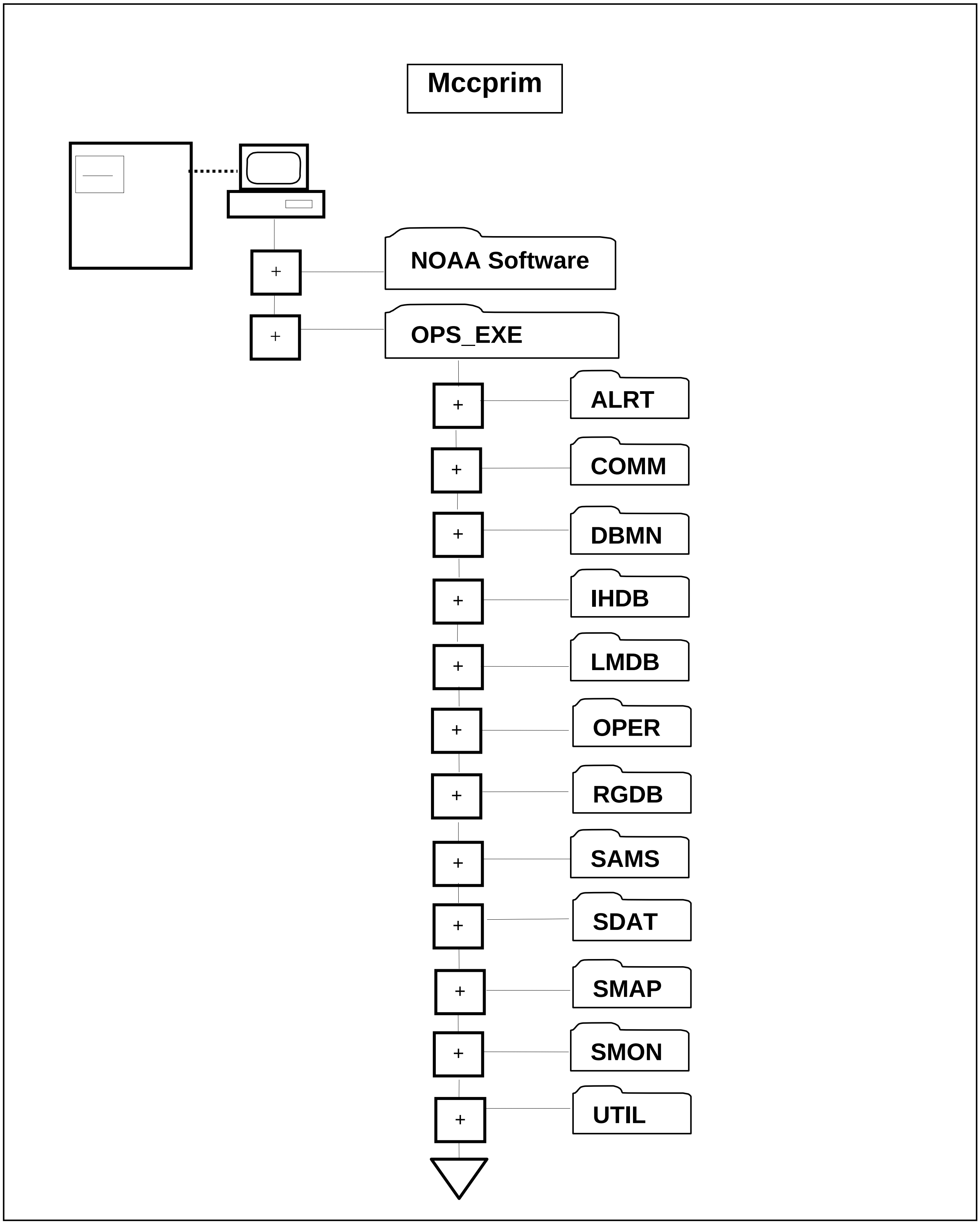


Figure 3.1: Application Software Directory Structure

3.1.2 Software Development Tools

Software development tools (e.g., compilers) used in the production of application software are under configuration control, the following products, as well as others, are under configuration management:

- MS Visual C++;
- MS Fortran;
- Intersolve;
- MS Visual Basic; and
- MS Enterprise Manager.
- JAVA

3.1.3 Commercial Off The Shelf Software (COTS)

All commercial off the shelf software required to support the USMCC and LUTs are also under configuration control. This includes, but is not limited to:

- all drivers required by application software (e.g., ODBC);
- all software fixes and updates (service packs, including dynamically linked libraries);
- MapInfo;
- Windows Operating System (2000, 2003 & XP);
- EICON software;
- Web Based COTs;
- Macromedia JRUN;
- J2E;
- Apache;
- Security COTs;
- ITS Real Secure Networks Sensor
- Audit Wizard;
- Shavlik;
- Backup COTS;
- Veritas;
- Backup Exec Server;
- Crystal Reports;
- Time Service;
- MapInfo;

3.1.4 Data Files

All data and configuration files (except those identified in section 3.3) used operationally by the USMCC are under configuration control. The location and access restrictions for data files is also under configuration control. These files include, but are not limited to:

- the Windows Registry in the USMCC;
- all binary files used by the USMCC;
- all ASCII files used by the USMCC;
- timers;
- all MS SQL Server tables used by the USMCC on an operational basis;
- all MS SQL Server Scripts used to generate tables.

3.1.5 Hardware

3.1.5.1 USMCC Network Equipment including:

- DMZ Segment Equipment
- MCC Segment Equipment

3.1.5.2 LUTServer Network Equipment including:

- LUT DMZ Segment Equipment
- LUT Intranet Segment Equipment
- LUT Server Segment Equipment;
- GEOLUT Segment Equipment

3.1.5.3 Web Applications Network Equipment including:

- Web DMZ Segment Equipment;
- Web Applications Segment Equipment

3.1.5.4 Offsite Network Equipment including:

- Offsite DMZ Segment Equipment;
- Offsite MCC Segment Equipment

The configuration status of the above equipment shall be maintained in the USMCC Functional Description Document (FDD).

3.1.6 Documentation

Documentation generated by DSD in support of the United States Cospas-Sarsat Program will be under configuration control. Documents describing requirements, interfaces, and descriptions are under configuration control. Documents include, but are not limited to:

- Functional Requirements Document;
- Functional Description Document;
- Detailed Description Document;
- Data Structures Document;
- Sarsat Security Plan
- RCC Messages Document;

- RCC Training Document;
- RCC Users Manual;
- IPD-DSD Interface Control Document;
- Telemetry and Command Procedures[1];
- Communications Description Document;
- National Coding Guidelines;
- Standard Operating Procedures;
- Interface Control Documents and
- Configuration Management Plan.

A comprehensive list of documentation is provided at:

\\MCCPRIM\DOCUMENTS\DOCUMENT.LST

The individual documents listed above, as well as other operational documents, are stored electronically according to the scheme provided in Figure

[1] Document is maintained by Canada (DnD), France (CNES) and the United States (NOAA/NASA)

3.2.

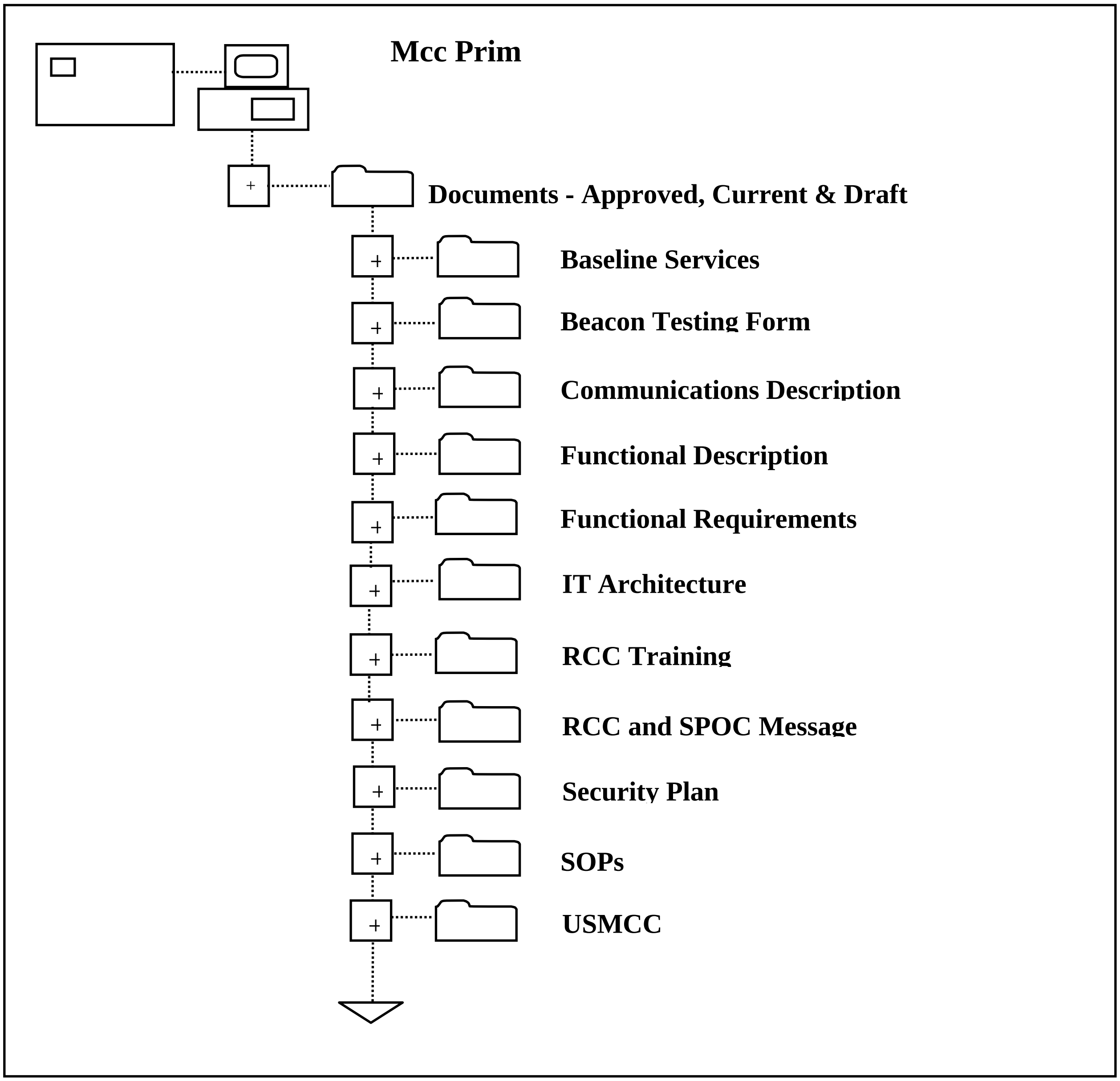


Figure 3.2: Document Directory Structure

3.2 LUTs

The configuration of individual software and hardware components of the LUTs is not maintained by DSD. However, all modifications are controlled through DSD configuration management. The communication equipment at the LUTs is maintained by the maintenance and operations vendor, and is included under the hardware described in section 3.1.5.

3.3 Items Not Included in Configuration Management

There are some configuration items used by USMCC operations that are not required to be under this configuration management plan. *Namely, configuration items that must be changed on short notice in response to changes in the operational environment are not required to be under this configuration management plan*. Insofar as this principle applies, the following configuration tables are not required to be this configuration management plan:

- AlertSite123SRR;
- AlertSite406SRR;
- AlertSite123Sum;
- AlertSite406Sum;
- Alert124FilterCfg (only for configuration to do with beacon exception processing);
- ComSiteCfg;
- ComEmailPathCfg (for routing only);
- ComX25PathCfg (for routing only);
- MccAlertRoutingCfg;
- MCCNOCRRoutingCfg;
- MidInfoCfg;
- SarRoutingCfg; and
- TelemSARPS?DigitalCfg, TelemSARRS?DigitalCfg (where ? = satellite number).

In addition, certain documentation is also not addressed by this configuration plan. This includes documentation used only by the operations staff, documentation developed and maintained by other organizations and used for reference by DSD (e.g., LUT documentation), and finally documentation that is maintained under the configuration control of another organization (e.g., Cospas-Sarsat documentation).

- End of Section 3 -

4 Change Control Procedures

Any change to an item, or an addition of an item, in the baselined system requires tracking using System Problem Reports (SPR) or System Change Proposals (SCP). SPRs are used to identify and initiate work to resolve a system problem. A system problem occurs when the system, or any of its components, malfunctions or does not meet defined requirements or specifications. SPRs are used to initiate corrective maintenance.

SCPs are used to propose changes, enhancements, or additions to the system. The change may be required to support adaptive or perfective maintenance. SCPs are also to be used to change system requirements or specifications. Figure 4.1 presents an overview of the change control procedures, and Figure 4.2 presents further details on the generation and use of SPRs and SCPs. Note that SPRs and SCPs can be generated by any person.

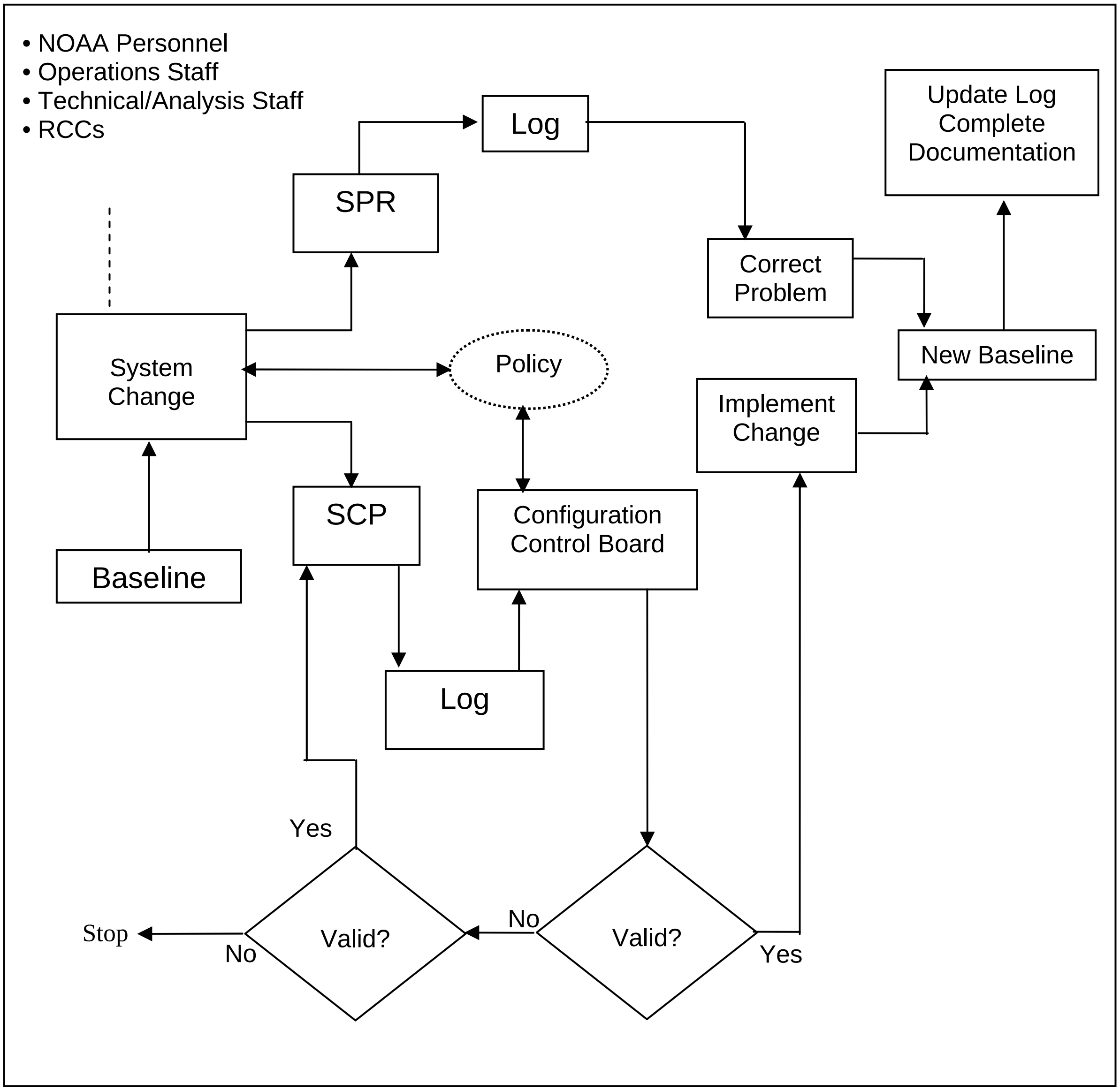
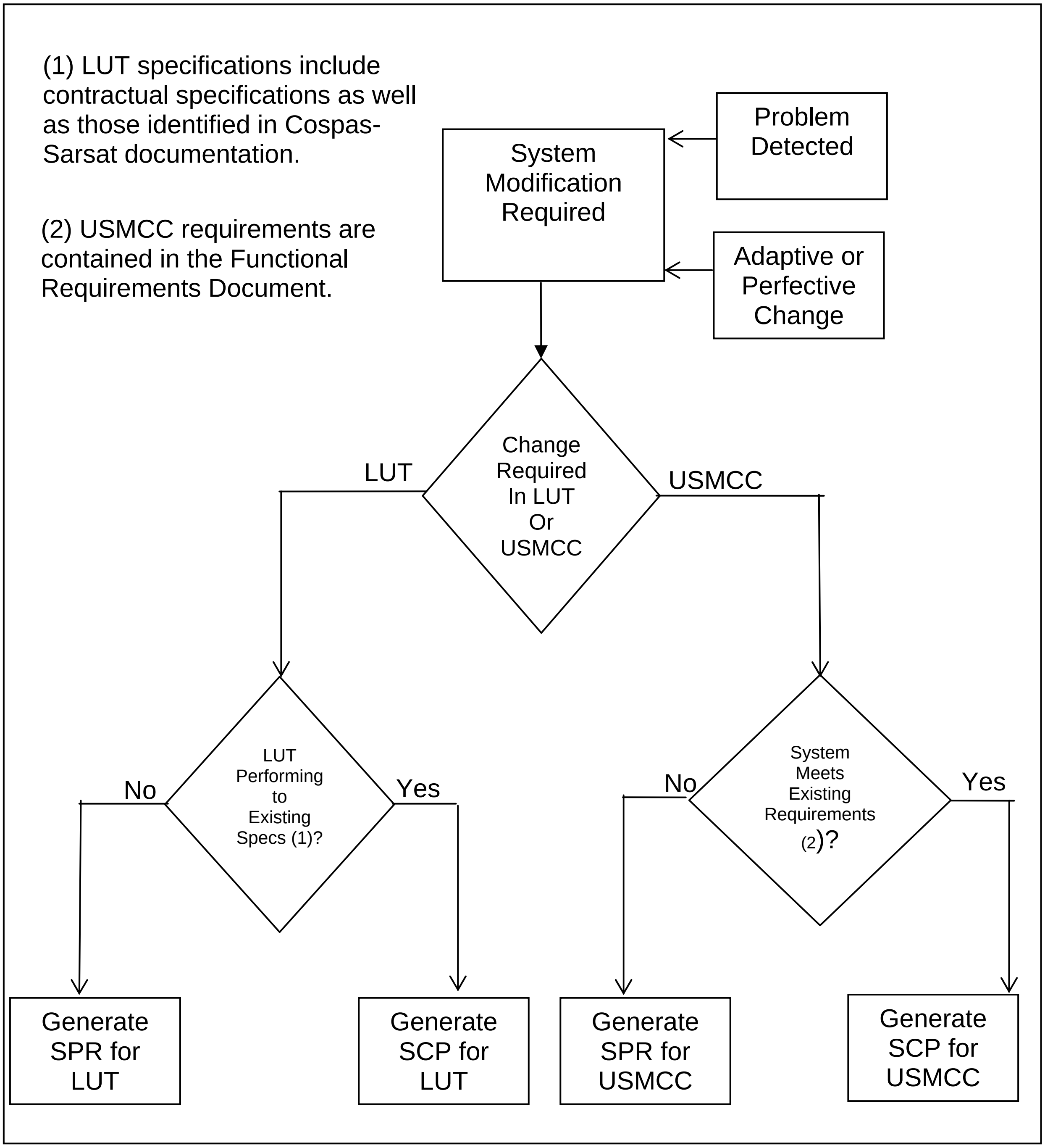


Figure 4.1:Overview of Change Control Procedures


Problem Detected
System Modification Required
Adaptive or Perfective Change
Change Required In LUT Or USMCC
LUT
USMCC
LUT Performing to Existing Specs (1)?
No
Yes
System Meets Existing Requirements (2)?
No
Yes
Generate SPR for LUT
Generate SCP for LUT
Generate SPR for USMCC
Generate SCP for USMCC

(1) LUT specifications include contractual specifications as well as those identified in Cospas-Sarsat documentation.

(2) USMCC requirements are contained in the Functional Requirements Document.

Figure 4.2: Use of SPRs and SCPs

4.1 System Problem Reports (SPR)

SPRs are typically generated by operational personnel as a result of routine monitoring or analysis. The anomalous system is identified and appropriate personnel notified. Procedures for notifying the LUT vendor regarding critical problems, or notifying supervisory personnel are contained in the Standard Operating Procedures.

Non-critical LUT problems should be reported to the LUT maintenance COTR for corrective action. All SPRs shall be reviewed by the Configuration Control Board after correction of the problem. Figure 4.3 describes the SPR process. Specific instructions can also be found in Section 6.

Critical problems for the LUT or the USMCC system are defined as anomalies that degrade the performance of the System so that search and rescue operations are impacted. For example:

- cause the loss of any alert data;
- cause a delay in the reception or transmission of alert data; or
- cause incorrect or invalid alert data to be transmitted.

Problems identified by external agencies (e.g., United States Air Force, United States Coast Guard, or other MCCs) should be reported to the SARSAT Operations Manager for initiation of a SPR.

4.2 System Change Proposals (SCP)

SCPs are generated by anyone to initiate adaptive or perfective maintenance. The appropriate system and subsystem(s) are identified, the objective and the justification for the change are provided on the SCP form (a blank form is provided at Appendix D).

For changes to the LUT system only the objective and justification for the change are required. The SCP should then be logged and submitted to the Configuration Control Board for further action. For changes to the USMCC system the person(s) performing the work, the estimated effort, and possible approaches to be used to implement the change should also be included. Figure 4.4 describes the initiation of a SCP. Specific instructions can also be found in section 6.

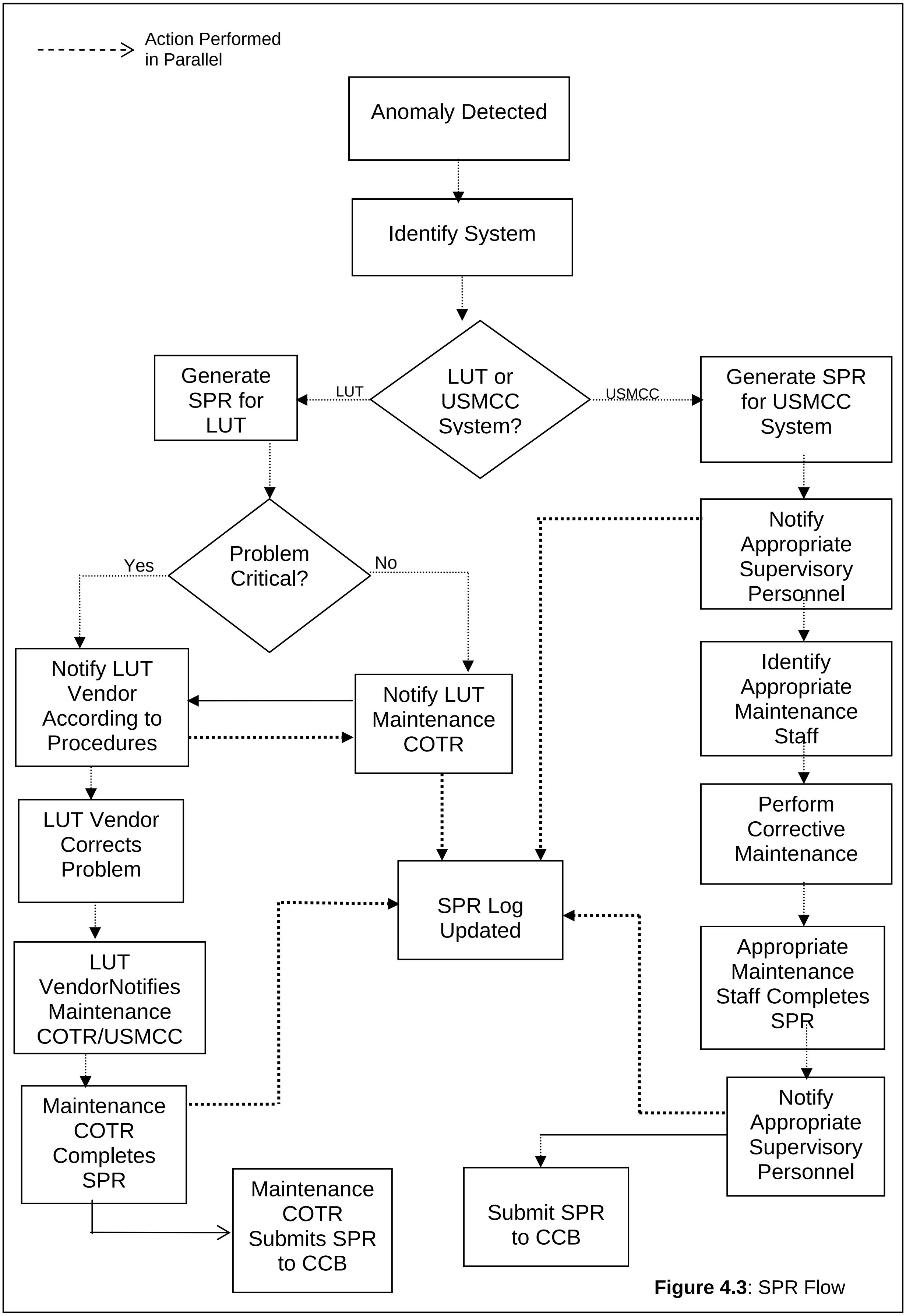

Action Performed in Parallel
Anomaly Detected
Identify System
LUT or USMCC System?
LUT
USMCC
Generate SPR for LUT
Generate SPR for USMCC System
Problem Critical?
Yes
No
Notify Appropriate Supervisory Personnel
Notify LUT Vendor According to Procedures
Notify LUT Maintenance COTR
Identify Appropriate Maintenance Staff
LUT Vendor Corrects Problem
Perform Corrective Maintenance
SPR Log Updated
LUT VendorNotifies Maintenance COTR/USMCC
Appropriate Maintenance Staff Completes SPR
Maintenance COTR Completes SPR
Notify Appropriate Supervisory Personnel
Maintenance COTR Submits SPR to CCB
Submit SPR to CCB

Figure 4.3: SPR Flow

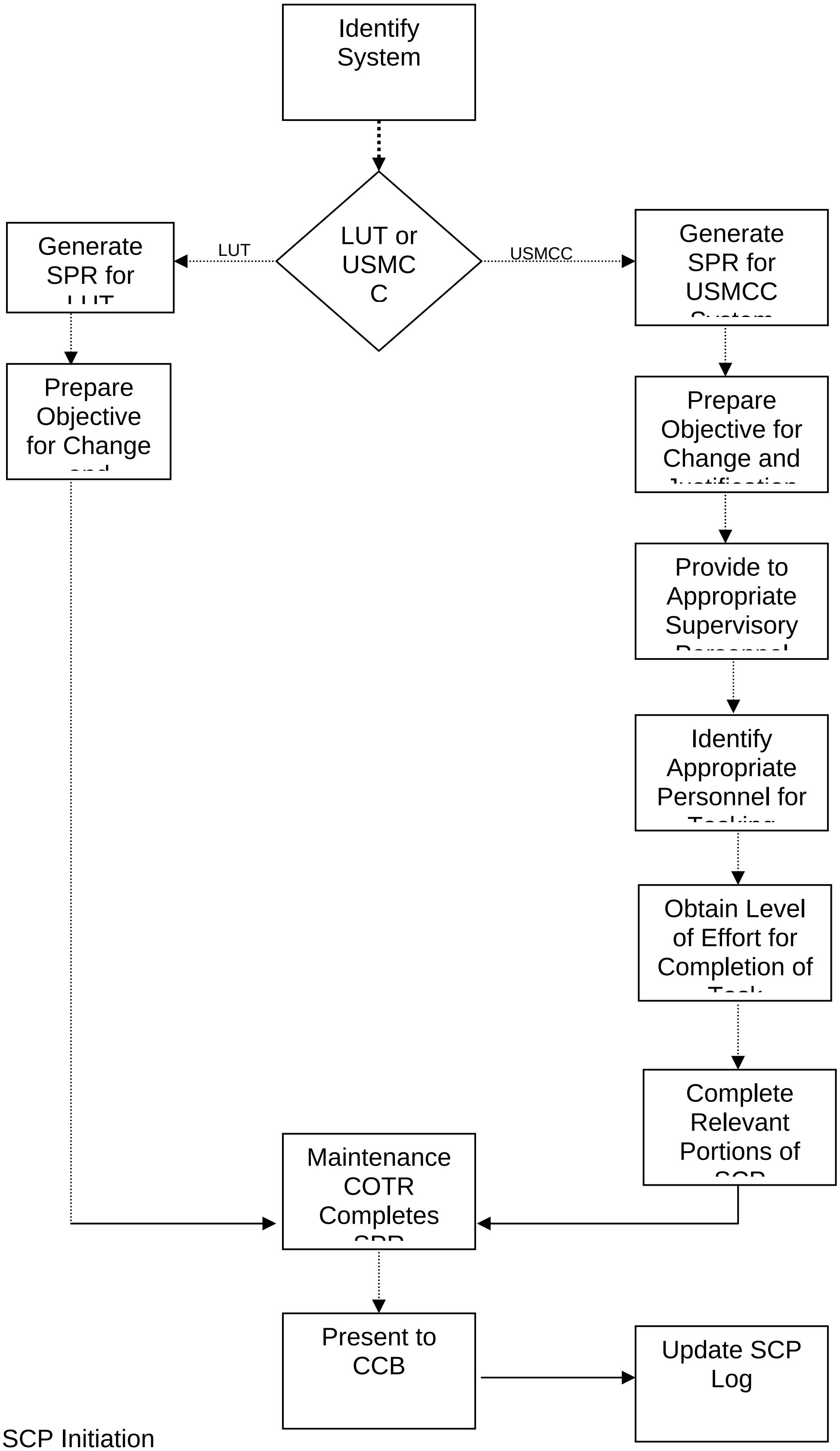

Identify System
LUT or USMCC
LUT
USMCC
Generate SPR for LUT
Generate SPR for USMCC System
Prepare Objective for Change and
Prepare Objective for Change and Justification
Provide to Appropriate Supervisory Personnel
Identify Appropriate Personnel for Tasking
Obtain Level of Effort for Completion of Task
Complete Relevant Portions of SCP
Maintenance COTR Completes SPR
Present to CCB
Update SCP Log

Figure 4.4: SCP Initiation

4.3 Configuration Control System (CCS)

The Configuration Control System (CCS) provides an automated interface and SQL based log to initiate, approve and monitor SCPs and SPRs. CCS details are provided in Appendix C.

4.4 Software Release Control

[To Be Developed - controls simultaneous updates of software, coordination of updating software at more than one site, and procedures for releasing software]

4.5 Software Version Control

[To Be Developed - identify unique versions of each software item, and identify versions of each software item which together constitute a specific version of a complete product]

4.6 Document Version Control

[To Be Develop]

- End of Section 4 -

5 Configuration Control Board

The configuration control board should meet as required to manage the configuration control process for the USMCC and LUT systems.

5.1 Authority

The configuration control board is responsible for reviewing completed and outstanding SPRs, and for reviewing, evaluating and approving SCPs. The configuration control board also evaluates reports and trends associated with the change control process, and administers this configuration management plan.

5.2 Membership

The membership of the configuration control board depends on the system(s) involved with the change. For changes to the USMCC system the following persons should be on the configuration control board as a minimum:

- Configuration Manager or designated representative;
- SARSAT Operations Manager or designated representative;
- Maintenance and Operations COTR or designated representative;
- USMCC Chief;
- Maintenance and Operations Administrative Representative; and
- Maintenance and Operations Senior Analyst or Lead Programmer (as required).
- ISSO

For changes to the LUT system the following persons should participate on the configuration control board as a minimum:

- Configuration Manager or designated representative;
- LUT Maintenance COTR or designated representative;
- SARSAT Operations Manager or designated representative;
- LUT Maintenance Vendor (as contractual agreements allow).
- ISSO

For both systems other persons (e.g., programmers, analysts, management) will be invited to participate as required.

5.3 Approval Process for SCPs

The change process is initiated by the submission of a SCP to the Configuration Manager who, after appropriate review and logging, distributes copies of the SCP to members of the configuration control board prior to the next meeting. The exception to the above being an SCP that is deemed URGENT by the initiator– in that case the SCP is to be immediately referred to the appropriate COTR for approval. The COTR, in evaluating the

SCP, will take into consideration its immediate operational impact and will either approve or reduce its status to routine in which case it will be reviewed at the CCB's next scheduled meeting. The configuration control board evaluates the request and determines whether the change should be approved. The determination is made by the respective COTRs considering the following factors:

- functional aspect of the change (e.g., consequences of not implementing change and complexity of change);
- current phase of the project;
- possible alternatives to the proposed change;
- resources required to implement change (time and cost);
- documentation requirements;
- integration and testing requirements;
- effect on other processing; and
- interface to other agencies/organizations.

Figure 5.1 describes the SCP approval process.

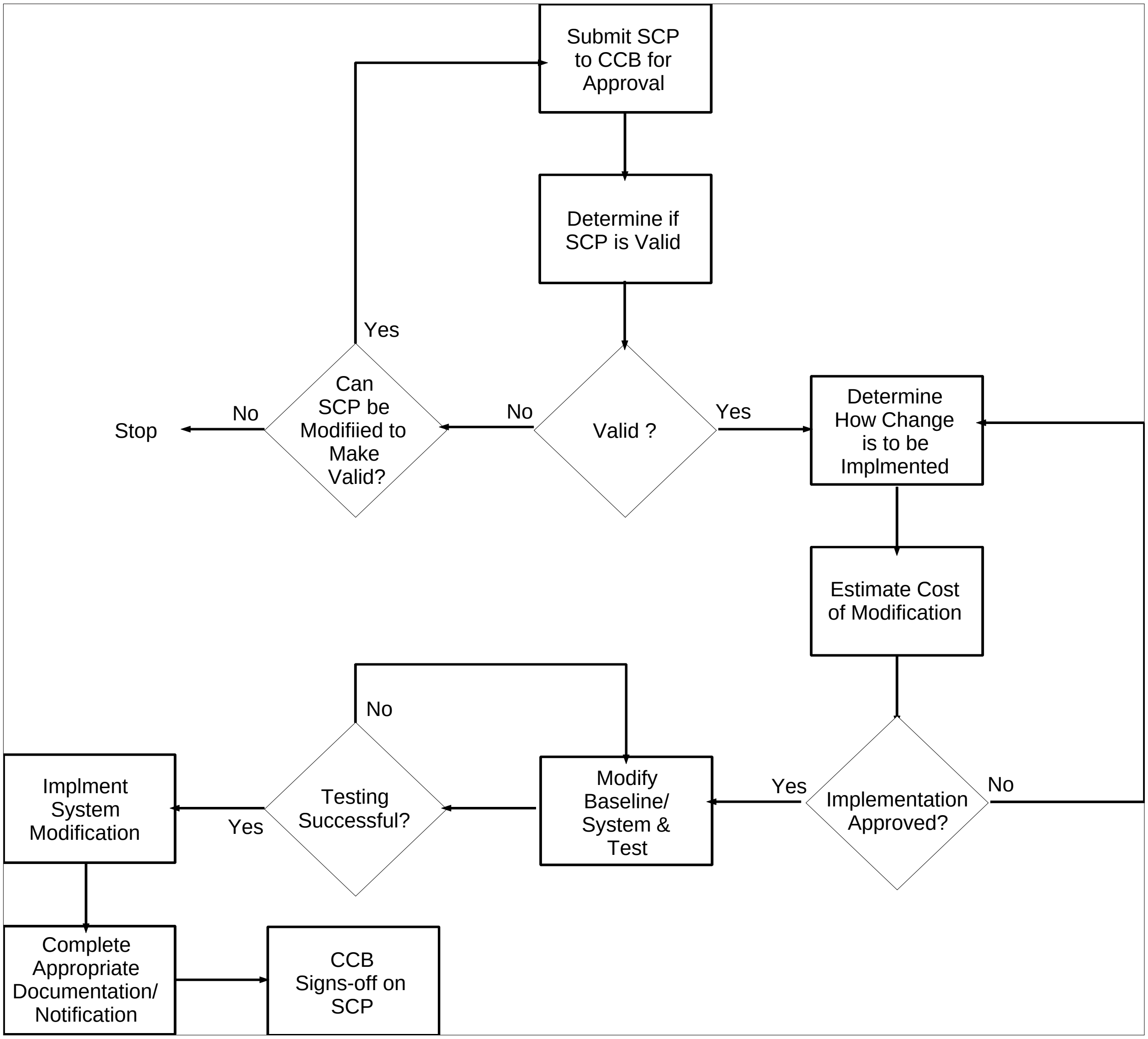

Submit SCP to CCB for Approval
Determine if SCP is Valid
Yes
Can SCP be Modifiied to Make Valid?
No
Stop
No
Valid ?
Yes
Determine How Change is to be Implmented
Estimate Cost of Modification
No
Implmentation Approved?
Yes
Modify Baseline/ System & Test
No
Testing Successful?
Yes
Implment System Modification
Complete Appropriate Documentation/ Notification
CCB Signs-off on SCP

Figure 5.1: Approval Process for SCPs

- End of Section 5 –

6 Configuration Control Tracking and Reporting

Modifications to the USMCC and LUT systems are tracked so that the configuration control board can assign priorities and ensure system problems are corrected, and proposed changes are properly tracked.

The current status and disposition of SPRs and SCPs will be tracked using the Configuration Control System (CCS) described at Appendix C. Separate databases exist for SPRs and SCPs. If a SPR or SCP is open one of the statuses described in Table 6.1 applies. If a SPR or SCP is closed one of the dispositions contained in Table 6.2 applies.

All SPRs and SCPs completed since the previous meeting of the configuration control board, and all open SPRs and SCPs will be reviewed by the configuration control board.

System Problem Report (SPR) **Status**	**System Change Proposal (SCP)** **Status**
No Work Performed - NW Work has not been initiated yet for this SPR.	Under Review - UR The SCP has been logged but has not been considered by the configuration control board
Design Phase - DP Modification to the system is being designed.	Design Phase - DP Modification to the system is being designed.
Coding Phase - CP Software is in the process of being modified. For hardware modifications, equipment is being modified or procured.	Coding Phase - CP Software is in the process of being modified. For hardware modifications, equipment is being modified or procured.
Test Phase - TP Modification is being tested.	Test Phase - TP Modification is being tested.
Implementation Phase - IP Modification is being integrated.	Implementation Phase - IP Modification is being integrated.
Documentation Phase - AP Appropriate documentation is being updated or created.	Documentation Phase - AP Appropriate documentation is being updated or created.
	On Hold - OH SCP reviewed, but on hold.

Table 6.1: Statuses of SPRs and SCPs

System Problem Report (SPR) **Disposition**	**System Change Proposal (SCP)** **Disposition**
Work Completed - WC Modification has been completed, integrated and all appropriate documentation updated.	Work Completed - WC Modification has been completed, integrated and all appropriate documentation updated.
Changed to SCP - CS After review SPR has been changed to an SCP	Changed to SPR - CS After review SCP has been changed to an SPR.
Not a Problem - NP After review it was determined that a problem did not exist.	SCP Not Approved - NA After review SCP was not approved.

Table 6.2: Disposition of SPRs and SCPs

The following reports will also be reviewed at least once a quarter:

- number of software modules under configuration control;
- number of SPRs and SCPs opened during the reporting period;
- number of SPRs and SCPs closed during the reporting period;
- average time to close SPRs and SCPs;
- mean time between failures and mean time to repair by subsystem; and
- number of SPRs and SCPs open greater than 60 days.

- ***End of Section 6 –***
-

Appendix A

Configuration Management Responsibilities

Configuration Manager	TBD Direct Services Division
ISSO	Wendy Holmes WSH Consulting
SARSAT Operations Manager	William Burkhart Direct Services Division
Maintenance and Operations COTR	William Burkhart Direct Services Division
LUT Maintenance COTR	Tom Button Direct Services Division
USMCC Chief	Sam Baker Science Systems and Applications, Inc.
Maintenance and Operations Project Manager	Joe Wagenhofer Science Systems and Applications, Inc.
Maintenance and Operations Senior Analyst/Lead Programmer	Tom Griffin Science Systems and Applications, Inc.
	Neil McConlogue Research and Profession Services

Appendix B

List of USMCC and LUT Systems

B.1 System: USMCC

Sub-System	Functions	Sub-System Identifier
Alert Processing	Validation, Match, Merge, Message Content, Destination	ALRT
Communication	Receipt, Formatting and Distribution of data.	COMM
System Data	Process Telemetry, Orbit Vectors, System Status, Spacecraft Commands, Time Calibration, Frequency Calibration, and Narrative Messages	SDAT
SAR Mapping	Perform Geosort and other Map Query functions	SMAP
System Monitoring	LUT Performance, MCC, Satellite, Large Location Error Reporting.	SMON
Operator Interface	Alert Site Query, Message Query, Operator Log	OPER
Database Maintenance	Archive, Purge, Backup, Database Performance	DBMN
Incident History Database	Entry, Report Generation of Incident data	IHDB
Registration Database	Entry, Confirmation, Report Generation of 406 MHz Registration data.	RGDB
Self-test and Monitoring	Availability, Performance, Statistical Reports	SAMS
LUT Monitoring Database	Availability, Contract Accounting	LMDB
Interference Monitoring	Interference Match/Merge, Report Generation	INTF

B.2 System: LUTs

[To Be Developed]

B.3 Documentation

List of USMCC and LUT documentation under configuration management is stored in file:

\\Mccprim\Document\Document_List

Appendix C

Configuration Control System

Configuration Control System (CCS)
System Description
20 September 2005

1. General

The terminology "Log" is used to refer to a given group of configuration management records, System Change Proposals (SCP) or System Problem Reports (SPR). The currently defined types of Logs are:

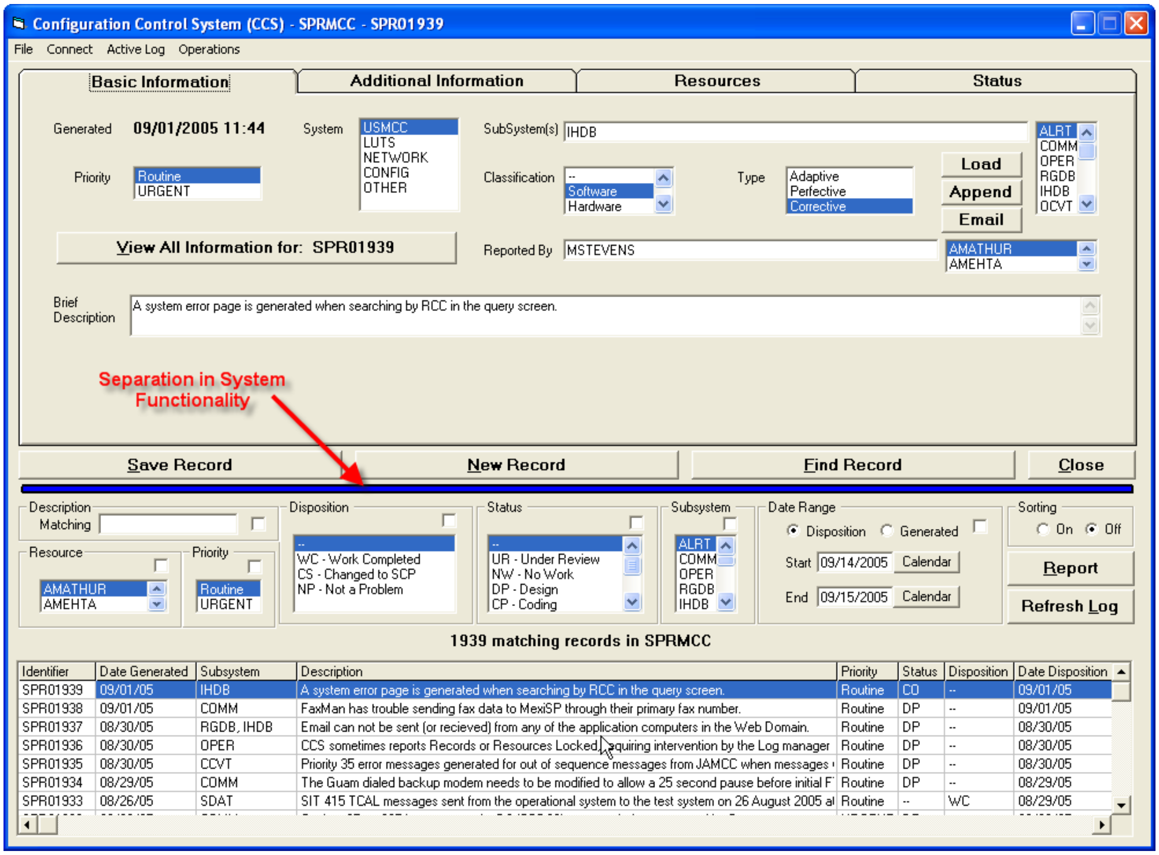
SCPMCC –SCPs for the USMCC
SPRMCC– SPRs for the USMCC
SCPDST – SCPs for the DST Web Applications
SPRDST – SPRs for the DST Web Applications
SCPLUT – SCPs for LUTs
SPRLUT – SPRs for LUTs

The types of Users of the CCS application are defined as follows:

View Only – Reviews records.
Auditor – Reviews records for accuracy and adherence to the process.
Resource – Does the work associated with a record and documents accordingly.
Log Manager – Oversees the ongoing work effort and record contents.
CCB Manager – Configuration Control Board (CCB), or an individual with the same level of control over the process, specifically approval and determination of final disposition for the record.

Figure 1 below shows the CCS Interface. As denoted, there are two main areas of functionality on the screen, divided by a dark blue band. The upper portion of the screen is for entering, modifying and displaying all the specific data fields associated with a given SCP or SPR. The four tabs are used to access various subsets of data. To the left, "Basic Information" and "Additional Information" describe the task. "Status", to the far right, is for tracking the approval process, the work in progress and the ultimate disposition of the record. The "Resources" tab provides fields for individuals who work on the tasks to record what was done, when it was done etc.

The area under the blue band predominately provides a mechanism for listing records that meet various settings in the filter criteria selected. The area at the very bottom of the screen provides a tabular listing with selected fields from these records. Above, the filter criteria is selected by first activating a given criteria with the associated check box and then selecting or entering the values to be matched or filtered upon. After selections are made a user clicks the "Refresh Log" button to list the matching records. Double-clicking on a record in this scrollable list, loads this record into the top half of the display. Finally, a button is also included here for running a canned report of activity related to records in the log. The only filter criterion that affects the content of the report is the "Date Range".



Generated 09/01/2005 11:44

System USMCC

SubSystem(s) IHDB

Priority Routine

Classification Software

Type Corrective

Reported By MSTEVENS

Brief Description A system error page is generated when searching by RCC in the query screen.

Separation in System Functionality

Date Range: Start 09/14/2005 End 09/15/2005

1939 matching records in SPRMCC

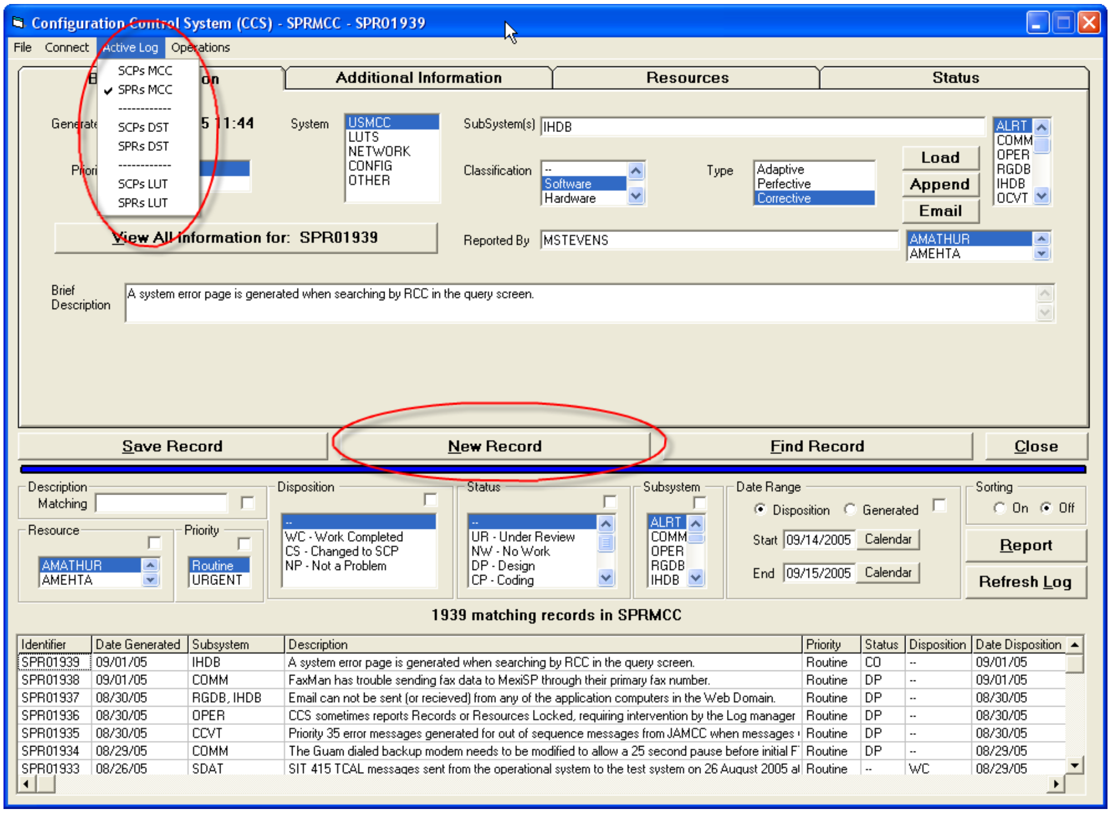
Identifier	Date Generated	Subsystem	Description	Priority	Status	Disposition	Date Disposition
SPR01939	09/01/05	IHDB	A system error page is generated when searching by RCC in the query screen.	Routine	CO	--	09/01/05
SPR01938	09/01/05	COMM	FaxMan has trouble sending fax data to MexiSP through their primary fax number.	Routine	DP	--	09/01/05
SPR01937	08/30/05	RGDB, IHDB	Email can not be sent (or recieved) from any of the application computers in the Web Domain.	Routine	DP	--	08/30/05
SPR01936	08/30/05	OPER	CCS sometimes reports Records or Resources Locked, requiring intervention by the Log manager	Routine	DP	--	08/30/05
SPR01935	08/30/05	CCVT	Priority 35 error messages generated for out of sequence messages from JAMCC when messages	Routine	DP	--	08/30/05
SPR01934	08/29/05	COMM	The Guam dialed backup modem needs to be modified to allow a 25 second pause before initial F	Routine	DP	--	08/29/05
SPR01933	08/26/05	SDAT	SIT 415 TCAL messages sent from the operational system to the test system on 26 August 2005 a	Routine	--	WC	08/29/05

Figure 1 - The CCS Interface

2. Description of the Basic Process

Step 1 – New Record is Added

Figure 2 below shows the CCS interface, highlighting the drop down menu to select the active log as well as the "New Record" button. New records are always defaulted to a status of "Under Review" (UR) and an "Approval Status" of unassigned (or pending). When a new record is added, a CCBManager (user with Approval capability for the given Log) is notified via an automated email. Typically, one or more LogManagers will also get a copy of the email. Records are created with no Resources yet assigned. The User who adds a record can also allocate Resources, but with some limitations which are detailed below in Section 3.



Generated 5 11:44

System: USMCC, LUTS, NETWORK, CONFIG, OTHER

SubSystem(s): IHDB

Classification: --, Software, Hardware

Type: Adaptive, Perfective, Corrective

Reported By: MSTEVENS

Brief Description: A system error page is generated when searching by RCC in the query screen.

Description Matching □

Resource □ AMATHUR, AMEHTA

Priority □ Routine, URGENT

Disposition □ --, WC - Work Completed, CS - Changed to SCP, NP - Not a Problem

Status □ --, UR - Under Review, NW - No Work, DP - Design, CP - Coding

Subsystem □ ALRT, COMM, OPER, RGDB, IHDB

Date Range: ● Disposition ○ Generated □

Start 09/14/2005

End 09/15/2005

Sorting: ○ On ● Off

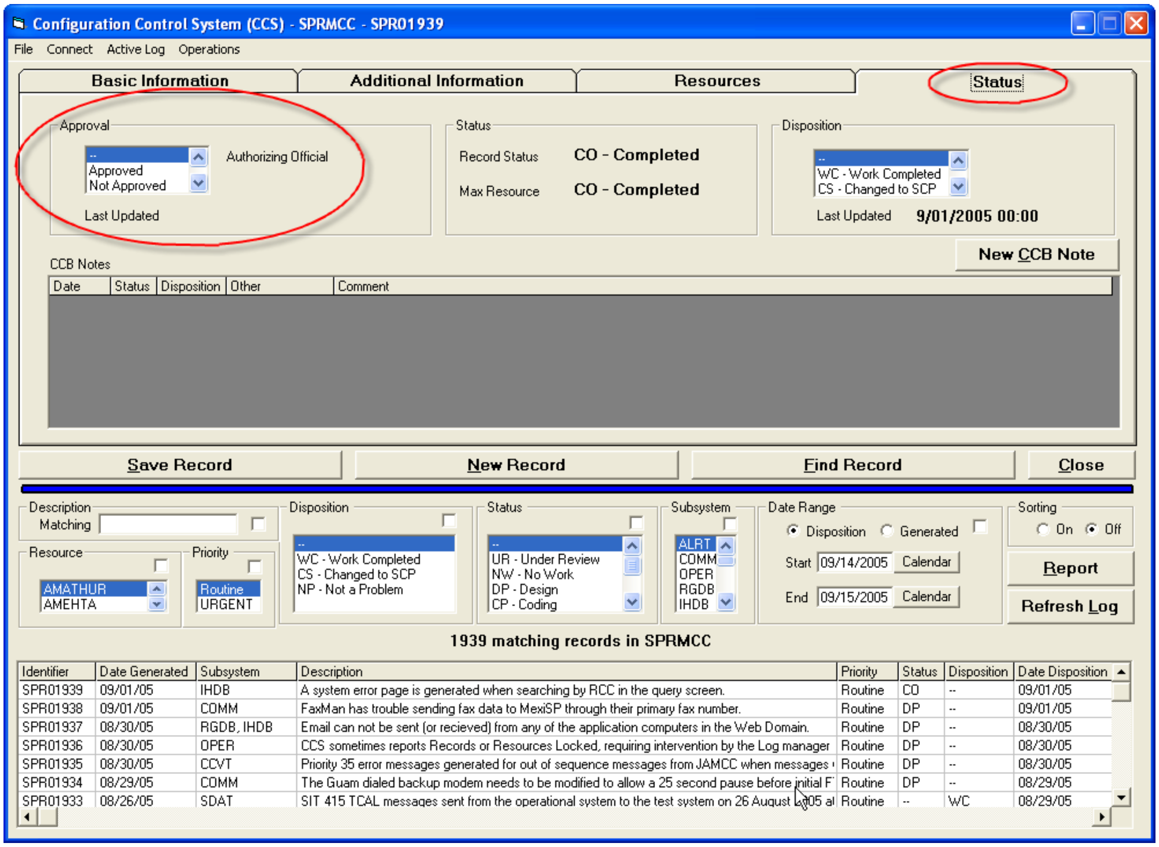
1939 matching records in SPRMCC

Identifier	Date Generated	Subsystem	Description	Priority	Status	Disposition	Date Disposition
SPR01939	09/01/05	IHDB	A system error page is generated when searching by RCC in the query screen.	Routine	CO	--	09/01/05
SPR01938	09/01/05	COMM	FaxMan has trouble sending fax data to MexiSP through their primary fax number.	Routine	DP	--	09/01/05
SPR01937	08/30/05	RGDB, IHDB	Email can not be sent (or recieved) from any of the application computers in the Web Domain.	Routine	DP	--	08/30/05
SPR01936	08/30/05	OPER	CCS sometimes reports Records or Resources Locked, requiring intervention by the Log manager	Routine	DP	--	08/30/05
SPR01935	08/30/05	CCVT	Priority 35 error messages generated for out of sequence messages from JAMCC when messages	Routine	DP	--	08/30/05
SPR01934	08/29/05	COMM	The Guam dialed backup modem needs to be modified to allow a 25 second pause before initial F	Routine	DP	--	08/29/05
SPR01933	08/26/05	SDAT	SIT 415 TCAL messages sent from the operational system to the test system on 26 August 2005 al	Routine	--	WC	08/29/05

Figure 2 – Generating a new record using CCS

<u>Step 2 – Approval</u>

When the CCBManager is notified of a new record, he/she reviews the record and approves or disapproves accordingly. In the case of SCPs, in particular routine ones, this approval may be done by committee (i.e., the CCB). The CCBManager can also add resources or modify the record itself as appropriate. When the record is updated (or saved) with the approval status set to "Approved", an email is automatically generated to each Resource associated with the record as well as the LogManager(s). Figure 3 below highlights the related areas.



Approval: -- / Approved / Not Approved
Authorizing Official
Last Updated

Status
Record Status CO - Completed
Max Resource CO - Completed

Disposition: -- / WC - Work Completed / CS - Changed to SCP
Last Updated 9/01/2005 00:00

CCB Notes

Date	Status	Disposition	Other	Comment

Description Matching □
Resource □ AMATHUR / AMEHTA
Priority □ Routine / URGENT
Disposition □ -- / WC - Work Completed / CS - Changed to SCP / NP - Not a Problem
Status □ -- / UR - Under Review / NW - No Work / DP - Design / CP - Coding
Subsystem □ ALRT / COMM / OPER / RGDB / IHDB
Date Range ● Disposition ○ Generated □
Start 09/14/2005
End 09/15/2005
Sorting ○ On ● Off

1939 matching records in SPRMCC

Identifier	Date Generated	Subsystem	Description	Priority	Status	Disposition	Date Disposition
SPR01939	09/01/05	IHDB	A system error page is generated when searching by RCC in the query screen.	Routine	CO	--	09/01/05
SPR01938	09/01/05	COMM	FaxMan has trouble sending fax data to MexiSP through their primary fax number.	Routine	DP	--	09/01/05
SPR01937	08/30/05	RGDB, IHDB	Email can not be sent (or recieved) from any of the application computers in the Web Domain.	Routine	DP	--	08/30/05
SPR01936	08/30/05	OPER	CCS sometimes reports Records or Resources Locked, requiring intervention by the Log manager	Routine	DP	--	08/30/05
SPR01935	08/30/05	CCVT	Priority 35 error messages generated for out of sequence messages from JAMCC when messages	Routine	DP	--	08/30/05
SPR01934	08/29/05	COMM	The Guam dialed backup modem needs to be modified to allow a 25 second pause before initial F	Routine	DP	--	08/29/05
SPR01933	08/26/05	SDAT	SIT 415 TCAL messages sent from the operational system to the test system on 26 August 2005 al	Routine	--	WC	08/29/05

Figure 3 - Status Tracking and Approval Process

Step 3 – Status Tracking

While the work effort associated with the record is "in progress", LogManagers and Resources can change the status of Resources as appropriate to track the progress. During this time, the record can be modified and Resources can be added or removed by a LogManager (or a CCBManager). Resources may add themselves, but only a User at the Manager level can add other individuals as Resources. An automated email will be generated if a Resource is newly added to a previous approved effort, but if other changes require the attention of Resources etc. the LogManager must notify the individual directly. During this time a Resource can also change their own area of information as desired to record on going efforts and track their individual status. Figure 3 above shows overall Status information and under the Resource tab individuals can specify their own individual status.

Step 4 – Work Completed

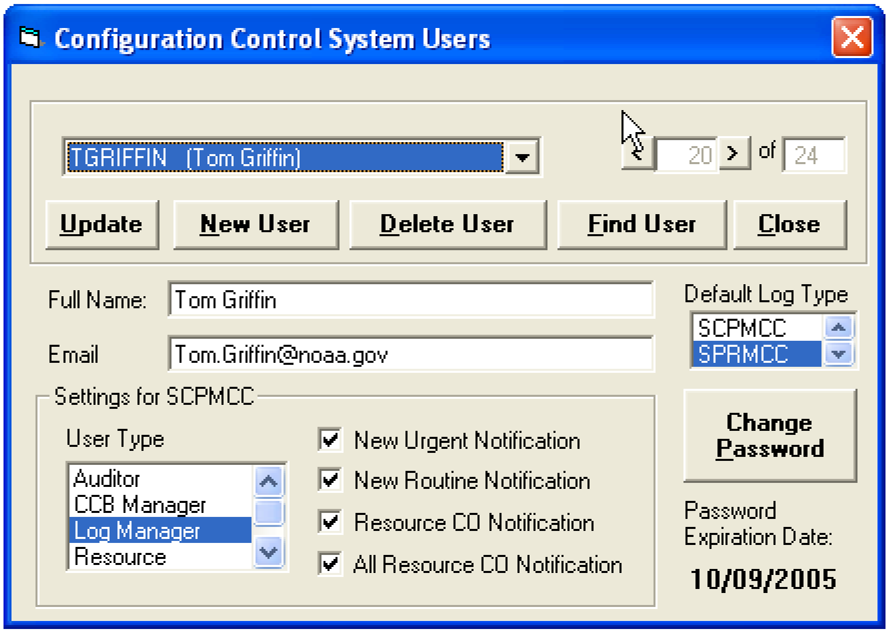
When a Resource is done their portion of the work effort (or all the work in the case of a single Resource record), he/she fills in all the fields in the Resource panel and accordingly sets the "Completed Date". The software will only allow the "Completed Date" to be set when all other required fields have been completed. When all Resources have reached this state, the software will automatically generate an email to the designated CCBManager (with a copy to the LogManager). Figure 3 above shows setting for Disposition including "Work Completed" (right hand side of the panel).

Step 5 – Record Completed

When the CCBManager has been notified that all work is complete (via automated email or otherwise), the general action is to verify that work and recorded information are all completed as appropriate, and change the final disposition to “Work Completed” (WC).

3. Managing Users and Related Configurations

The CCS Interface employs several configuration tables to manage Users, storing login names, encrypted passwords, email addresses etc. as well as various permissions pertaining to specific functions. Facilities are provided for Log Managers and CCB Managers to configure these settings. Section 1 above outlines the basic User types. Figure 4 below denotes the CCS interface dialog box which provids for setting User configurations (accessed by selecting the appropriate option from the “Operations” drop down menu from the main window).



Configuration Control System Users

TGRIFFIN (Tom Griffin)

20 of 24

Full Name: Tom Griffin

Email Tom.Griffin@noaa.gov

Default Log Type
SCPMCC
SPRMCC

Settings for SCPMCC

User Type
Auditor
CCB Manager
Log Manager
Resource

☑ New Urgent Notification
☑ New Routine Notification
☑ Resource CO Notification
☑ All Resource CO Notification

Password Expiration Date: 10/09/2005

Figure 4 - Configuring CCS Users

Several settings for users are general, such as the login name (e.g., TGRIFFIN), password and Default Log Type and some are log specific such as the User Type and check boxes for Email Notifications. Settings are made for a specific log by selecting the Active Log from the “Active Log” drop down menu (See Figure 2) before opening the above dialog box. The specific permissions associated with the five User types are detailed in Table 1 below.

	May Add Records	May Add Self As Resource	May Edi t Self As Resource	May Add / Remove Resources	May Edit Resources	May Change Records After Approval	May Change Disposition	May Approve Records	May Edit After Disposition Set	May Manage Users	May Create CCB Notes
View Only											
Auditor	X										
Resource	X	X	X								
Log Manager	X	X	X	X	X	X				X	
CCB Manager	X	X	X	X	X	X	X	X	X	X	X

Table 1 – Permissions by User Type